明細書

被認証装置及び認証装置及び認証方法

技術分野

本発明は、被認証装置、或いは認証装置に関する。または、上記認証装置と上記被認証装置との間で認証をおこなう認証方法に関する。

背景技術

利用者があるサービスを受けるとき、サービスを受けられる正当な利用者であるかどうか本人確認（認証）が行なわれ、暗号通信のための鍵共有が行なわれる。暗号通信に用いられる暗号アルゴリズムは１種類であり、異なるアルゴリズムを実装している装置間では認証及び鍵共有が行えない。

また、複数の暗号技術利用プロトコルの利用が可能な通信システムについての記載が載った文献が存在する（特開平１０－３０４３３３号公報）。

また、複数のアルゴリズムを用いた技術についての記載が載った文献が存在する（特開２０００－１５１５７８号公報，特開平５－２２７１５２号公報）。

以上のように、従来は、暗号通信に用いられる暗号アルゴリズムは１種類であるため、アルゴリズムの脆弱性が発見されたり、解読されたり、鍵の漏洩等によりデータ暗号化によるセキュリティ（安全）が保たれなくなった場合に、より安全なアルゴリズム等を実装することになるが、これにより装置間で異なるアルゴリズムを実装する場合が生じ、上述したように異なるアルゴリズムを実装している装置間では認証及び鍵共

有が行えないといった問題があった。また、各メーカ等がそれぞれ販売等している暗号アルゴリズムがあるために、異なるアルゴリズムを実装している装置間では認証及び鍵共有が行なえないといった問題があった。

また、上述したようにセキュリティ（安全）が保たれなくなった場合に、より安全なアルゴリズムを実装することになるが、新たなアルゴリズム等を実装することによりそれまでのシステム及び装置が使い物にならなくなるといった問題があった。

また、将来、より高度なアルゴリズムが考案されたとしてもそれまで使用していた装置に適用することができないといった問題があった。

本発明は、搭載しているアルゴリズムが異なるために認証が行なえないといった問題を解決することを目的とする。

本発明は、１つのアルゴリズムが解読等により使用できなくなっても引き続きシステム及び装置を運用可能とすることを目的とする。

また、本発明は、引き続きシステム及び装置を運用可能とすることで、アルゴリズムの解読等によるセキュリティ低下というリスクを軽減することを目的とする。

また、本発明は、盗聴等による不正な解読等の機会を減らし、セキュリティを向上させることを目的とする。

発明の開示

この発明に係る被認証装置は、少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを記憶する記憶部と、

上記記憶部により記憶された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを認証装置に送信する送信部と、

上記認証装置から上記送信部により送信された少なくとも１つのアル

ゴリズム識別子と少なくとも１つの暗号鍵識別子との中から選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する受信部と、

上記受信部により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子に基づいて上記認証装置との間で認証処理をおこなう認証処理部と

を備えたことを特徴とする。

また、上記記憶部は、１つのアルゴリズム識別子と１つの暗号鍵識別子とを１組のプロファイルとして、少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを記憶し、

上記送信部は、上記記憶部により１つのアルゴリズム識別子と１つの暗号鍵識別子とを１組のプロファイルとして記憶された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを認証装置に送信し、

上記受信部は、上記認証装置から上記送信部により送信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子との中から所定のプロファイルとして組となる上記所定のアルゴリズム識別子と上記所定の暗号鍵識別子とを受信し、

上記認証処理部は、上記受信部により受信された所定のプロファイルとして組となる所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置との間で認証処理をおこなうことを特徴とする。

また、上記記憶部は、さらに、記憶された少なくとも１つのアルゴリズム識別子に対応する少なくとも１つのアルゴリズムを１つのセットとした上記セットを示すバージョンを識別するバージョン識別子を記憶し、

上記送信部は、上記記憶部により記憶されたバージョン識別子を認証

装置に送信し、

上記受信部は、上記認証装置から上記送信部により送信されたバージョン識別子が識別するバージョンが示すセットとなる少なくとも１つのアルゴリズムの中の所定のアルゴリズムに対応する上記所定のアルゴリズム識別子を受信し、

上記認証処理部は、上記受信部により受信された所定のアルゴリズム識別子と上記所定のアルゴリズム識別子と組となる所定の暗号鍵識別子とに基づいて上記認証装置との間で認証処理をおこなうことを特徴とする。

また、この発明に係る認証装置は、少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを記憶する記憶部と、

被認証装置から少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを受信する受信部と、

上記受信部により受信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子との中に上記記憶部により記憶された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とが存在する場合に、上記受信部により受信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子との中から上記記憶部により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択する選択部と、

上記選択部により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記被認証装置に送信する送信部と、

上記送信部により送信される所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記被認証装置との間で認証処理をおこなう認証処理部と

を備えたことを特徴とする。

また、上記記憶部は、少なくとも１つのアルゴリズム識別子の１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子の１つの暗号鍵識別子とを組とする少なくとも１つのプロファイルを識別する少なくとも１つのプロファイル識別子を記憶し、

上記受信部は、さらに、上記被認証装置から少なくとも１つのプロファイル識別子を受信し、

上記選択部は、上記受信部により受信された少なくとも１つのプロファイル識別子の中に上記記憶部により記憶された少なくとも１つのプロファイル識別子が存在する場合に、上記受信部により受信された少なくとも１つのプロファイル識別子の中から上記記憶部により記憶される所定のプロファイル識別子を選択し、

上記送信部は、上記選択部により選択された所定のプロファイル識別子を上記被認証装置に送信し、

上記認証処理部は、上記送信部により送信される所定のプロファイル識別子により識別される所定のプロファイルが組とする上記所定のアルゴリズム識別子と上記所定の暗号鍵識別子とに基づいて上記被認証装置との間で認証処理をおこなうことを特徴とする。

また、上記記憶部は、さらに、記憶された少なくとも１つのアルゴリズム識別子に対応する少なくとも１つのアルゴリズムを１つのセットとして、上記セットのバージョンを識別するバージョン識別子を記憶し、

上記受信部は、さらに、上記被認証装置から所定のバージョン識別子を受信し、

上記選択部は、上記受信部により受信された所定のバージョン識別子が識別するバージョンが示すセットの中の１つのアルゴリズムに対応する上記所定のアルゴリズム識別子を選択し、

上記送信部は、上記選択部により選択された所定のアルゴリズム識別

子を上記被認証装置に送信し、

上記認証処理部は、上記送信部により送信される所定のアルゴリズム識別子と上記所定のアルゴリズム識別子と組となる所定の暗号鍵識別子とに基づいて上記被認証装置との間で認証処理をおこなうことを特徴とする。

この発明に係る認証方法は、複数のアルゴリズム識別子と複数の暗号鍵識別子とを記憶する被認証装置から記憶された複数のアルゴリズム識別子と複数の暗号鍵識別子とを認証装置に送信する第１の送信工程と、

少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを記憶する認証装置が、上記第１の送信工程により被認証装置から送信された複数のアルゴリズム識別子と複数の暗号鍵識別子とを受信する第１の受信工程と、

上記第１の受信工程により受信された複数のアルゴリズム識別子と複数の暗号鍵識別子との中に上記認証装置により記憶された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とが存在する場合に、上記認証装置が上記受信工程により受信された複数のアルゴリズム識別子と複数の暗号鍵識別子との中から上記認証装置により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択する選択工程と、

上記選択工程により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置から上記被認証装置に送信する第２の送信工程と、

上記被認証装置が上記認証装置から上記第２の送信工程により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する第２の受信工程と、

上記第２の受信工程により受信された所定のアルゴリズム識別子と所

定の暗号鍵識別子とに基づいて上記認証装置と上記被認証装置との間で認証処理をおこなう認証処理工程とを備えたことを特徴とする。

また、この発明に係る認証方法は、少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを記憶する被認証装置から記憶された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを認証装置に送信する第１の送信工程と、

複数のアルゴリズム識別子と複数の暗号鍵識別子とを記憶する認証装置が、上記第１の送信工程により被認証装置から送信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを受信する第１の受信工程と、

上記第１の受信工程により受信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子との中に上記認証装置により記憶された複数のアルゴリズム識別子の少なくとも１つと複数の暗号鍵識別子の少なくとも１つとが存在する場合に、上記認証装置が上記受信工程により受信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子との中から上記認証装置により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択する選択工程と、

上記選択工程により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置から上記被認証装置に送信する第２の送信工程と、

上記被認証装置が上記認証装置から上記第２の送信工程により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する第２の受信工程と、

上記第２の受信工程により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置と上記被認証装置との間で認証処理をおこなう認証処理工程とを備えたことを特徴とする。

図面の簡単な説明

図１は、実施の形態１における認証システムの構成を示す図である。

図２は、実施の形態１における認証方法を示すフローチャート図である。

図３は、通信情報１のフレームの一例を示す図である。

図４は、通信情報２のフレームの一例を示す図である。

図５は、通信情報３のフレームの一例を示す図である。

図６は、通信情報４のフレームの一例を示す図である。

図７は、通信装置２００側に搭載されているアルゴリズム識別子と暗号鍵識別子とアルゴリズムと個別鍵とを示す図である。

図８は、通信装置１００側に搭載されているアルゴリズム識別子と暗号鍵識別子とアルゴリズムとを示す図である。

図９は、実施の形態２における認証システムの構成を示す図である。

図１０は、実施の形態２における認証方法を示すフローチャート図である。

図１１は、実施の形態３における認証方法を示すフローチャート図である。

図１２は、実施の形態４における認証方法を示すフローチャート図である。

図１３は、実施の形態５における認証方法を示すフローチャート図である。

図１４は、ハードウェア構成図である。

発明を実施するための最良の形態

実施の形態１.

図１は、実施の形態１における認証システムの構成を示す図である。

図１において、認証システムは、認証装置となる通信装置１００と被認証装置となる通信装置２００とを備えている。通信装置１００は、アンテナ１０１、通信処理部１１０、記憶部１２０、制御部１３０、選択部１６０、認証処理部１９６を備えている。通信処理部１１０は、受信部１１１、送信部１１２を有している。認証処理部１９６は、暗号処理部１４０、乱数生成部１５０、個別鍵生成部１７０、一時鍵生成部１８０、認証用データ１生成部１９０、認証用データ２チェック部１９５を有している。通信装置２００は、アンテナ２０１、通信処理部２１０、記憶部２２０、制御部２３０、認証処理部２９６を備えている。通信処理部２１０は、受信部２１１、送信部２１２を有している。認証処理部２９６は、暗号処理部２４０、乱数生成部２５０、一時鍵生成部２８０、認証用データ１チェック部２９０、認証用データ２生成部２９５を有している。実施の形態１では、通信装置１００と通信装置２００とは、アンテナ１０１，２０１を介して無線通信する場合を説明するが、これに限るものではなく有線通信であっても構わない。例えば、ＥＴＣ（料金自動収集）、ドライブスルー等において、通信装置１００は、店舗側の路側機として、通信装置２００は、自動車側の車載機として構成される。

図２は、実施の形態１における認証方法を示すフローチャート図である。

記憶部１２０は、少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子と、上記少なくとも１つのアルゴリズム識別子の各アルゴリズム識別子に対応するアルゴリズムを記憶している。また、上記記憶部１２０は、少なくとも１つのアルゴリズム識別子の１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子の１つの暗号鍵識別子

とを組とする少なくとも１つのプロファイルを識別する少なくとも１つのプロファイル識別子を記憶している。

記憶部２２０は、少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子と、上記少なくとも１つのアルゴリズム識別子の各アルゴリズム識別子に対応するアルゴリズムと上記少なくとも１つの暗号鍵識別子の各暗号鍵識別子に対応する暗号鍵となる装置固有の個別鍵と装置固有番号とを記憶している。また、上記記憶部２２０は、１つのアルゴリズム識別子と１つの暗号鍵識別子とを１組のプロファイルとして、少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とプロファイルを識別する少なくとも１つのプロファイル識別子とを記憶している。

ここで、通信装置１００，２００のうち、少なくとも一方において、アルゴリズム識別子と暗号鍵識別子との組が複数存在すればよい。

Ｓ（ステップ）２０１において、認証処理工程の一部として、乱数生成部１５０は、乱数１を生成する。

Ｓ２０２において、送信工程として、送信部１１２は、乱数生成部１５０により生成された乱数１を通信情報１として通信装置２００に送信する。例えば、通信装置２００を搭載した自動車が、通信装置１００により図示していない検知器により検知された場合に、送信部１１２は、乱数１を通信装置２００に送信する。通信装置１００は、乱数１を通信情報１として通信装置２００に送信することで、通信装置２００が保持している鍵情報（鍵識別子、アルゴリズム識別子）を要求する。言い換えれば、通信情報１が通信装置２００への要求情報となる。

Ｓ２０３において、受信工程として、受信部２１１は、送信部１１２により送信された乱数１を通信情報１として受信する。通信装置２００では、受信部２１１が、乱数１を受信したことにより、通信装置１００

より通信装置２００が保持している鍵情報（鍵識別子、アルゴリズム識別子）が要求されたと判断する。

Ｓ２０４において、認証処理工程の一部として、乱数生成部２５０は、乱数２を生成する。

Ｓ２０５において、送信工程（第１の送信工程）として、送信部２１２は、上記記憶部２２０により記憶された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子と装置固有番号と、乱数生成部２５０により生成された乱数２とを通信情報２として認証装置である通信装置２００に送信する。ここで、１つのアルゴリズム識別子と１つの暗号鍵識別子とを１組みとしてプロファイルとして表し、通信情報２は、乱数２と装置固有番号と組数分のプロファイル数とプロファイル数分の各プロファイル識別子と各プロファイル識別子が表すプロファイルに組とされるアルゴリズム識別子と暗号鍵識別子とをデータとして有している。さらに、ここでは、各プロファイル識別子と各プロファイル識別子が表すプロファイルに組とされるアルゴリズム識別子と暗号鍵識別子とを対応させたデータとしている。言い換えれば、上記送信部２１２は、上記記憶部２２０により１つのアルゴリズム識別子と１つの暗号鍵識別子とを１組のプロファイルとして記憶された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを認証装置となる通信装置１００に送信する。

Ｓ２０６において、受信工程（第１の受信工程）として、受信部１１１は、被認証装置となる通信装置２００から、乱数２と装置固有番号と組数分のプロファイル数とプロファイル数分の少なくとも１つのプロファイル識別子と少なくとも１つのプロファイル識別子の各プロファイル識別子に対応した少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを有する通信情報２を受信する。

Ｓ２０７において、選択工程として、選択部１６０は、上記受信部１１１により受信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子との中に上記記憶部１２０により記憶された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とが存在する場合に、上記受信部１１１により受信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子との中から上記記憶部１２０により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択する。言い換えれば、上記選択部１６０は、上記受信部１１１により受信された少なくとも１つのプロファイル識別子の中に上記記憶部１２０により記憶された少なくとも１つのプロファイル識別子が存在する場合に、上記受信部１１１により受信された少なくとも１つのプロファイル識別子の中から上記記憶部１２０により記憶される所定のプロファイル識別子を選択する。所定のプロファイル識別子を選択することで、所定のプロファイル識別子が示すプロファイルに組みする所定のアルゴリズム識別子と所定の暗号鍵識別子とが選択される。例えば、単純に、通信装置１００，２００双方が共通して有しているアルゴリズム識別子と暗号鍵識別子とを選択してもよいし、暗号解読等により既にセキュリティが十分でなくなったアルゴリズム識別子と暗号鍵識別子とを排除した上で、通信装置１００，２００双方が共通して有しているアルゴリズム識別子と暗号鍵識別子とを選択してもよい。また、実施の形態１では、所定のプロファイル識別子を選択することで、所定のプロファイル識別子に対応するアルゴリズム識別子と暗号鍵識別子とを選択する。

Ｓ２０８において、認証処理工程の一部として、個別鍵生成部１７０は、上記選択部１６０により選択された所定の暗号鍵識別子に対応する暗号鍵となる通信装置２００が有している個別鍵を通信情報２の装置固

有番号から例えばハッシュ値等を用いて生成する。

Ｓ２０９において、認証処理工程の一部として、一時鍵生成部１８０は、上記選択部１６０により選択された所定のアルゴリズム識別子に対応するアルゴリズムを用いて所定の暗号鍵識別子に対応する暗号鍵となる個別鍵生成部１７０により生成された個別鍵で乱数１，２を暗号処理部１４０を用いて暗号化し、認証処理用暗号鍵の一例となる一時鍵を生成する。

Ｓ２１０において、認証処理工程の一部として、認証用データ１生成部１９０は、乱数２のすべて或いは一部を暗号処理部１４０により一時鍵生成部１８０により生成された一時鍵で暗号化することにより認証用データ１を生成する。

Ｓ２１１において、送信工程（第２の送信工程）として、送信部１１２は、上記選択部１６０により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子と上記選択部により選択された対応する所定のプロファイル識別子と認証用データ１生成部１９０により生成された認証用データ１とを通信情報３として上記被認証装置となる通信装置２００に送信する。

Ｓ２１２において、受信部２１１は、上記認証装置となる通信装置１００から上記送信部２１２により送信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子との中から選択された所定のアルゴリズム識別子と所定の暗号鍵識別子と所定のアルゴリズム識別子と所定の暗号鍵識別子と対応するプロファイル識別子と認証用データ１とを通信情報３として受信する。言い換えれば、上記受信部２１１は、上記認証装置となる通信装置１００から上記送信部２１２により送信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子との中から所定のプロファイルとして組となる所定のアルゴリズ

ム識別子と所定の暗号鍵識別子とを受信する。

Ｓ２１３において、認証処理工程の一部として、暗号処理部２４０は、受信部２１１により受信されたプロファイル識別子を確認し、プロファイル識別子に対応する所定の暗号鍵識別子と所定のアルゴリズム識別子とを確認する。

Ｓ２１４において、認証処理工程の一部として、一時鍵生成部２８０は、受信部２１１により受信され、暗号処理部２４０により確認された所定のアルゴリズム識別子に対応するアルゴリズムを用いて、記憶部２２０に記憶された個別鍵で乱数１，２を暗号処理部２４０を用いて暗号化し、認証処理用暗号鍵の一例となる上記一時鍵を生成する。以上により通信装置１００，２００間で同じ一時鍵という鍵共有ができたことになる。なお、記憶部２２０に記憶された個別鍵は、個別鍵生成部１７０と同様の生成方法で生成されたものであり、あらかじめ、ＩＣカード等何かしらの手段を用いて記憶部２２０に記録されている。なお、この実施形態では、一時鍵生成部１８０，２８０が一時鍵生成の際、個別鍵で暗号化したが、認証装置と被認証装置とが同じ処理を実施すればよいため、復号してもよい。

Ｓ２１５において、認証処理工程の一部として、認証用データ１チェック部２９０は、受信部２１１により通信情報３として受信された暗号化されている認証用データ１を一時鍵生成部２８０により生成された一時鍵により暗号処理部２４０を用いて復号する。

Ｓ２１６において、認証処理工程の一部として、認証用データ１チェック部２９０は、復号した認証用データ１のデータが、通信装置２００が通信装置１００に送信した乱数２のすべて或いは一部であるかどうかを確認する。復号した認証用データ１のデータが乱数２のすべて或いは一部であれば、不正の攻撃者との間ではなく、通信装置１００との間で

認証処理のための通信がきちっと行なわれていることを意味する。言い換えれば、通信装置１００，２００間での認証処理の一方が成功したことを意味する。

Ｓ２１７において、認証処理工程の一部として、認証用データ２生成部２９５は、乱数１のすべて或いは一部を暗号処理部２４０により一時鍵生成部２８０により生成された一時鍵で暗号化することにより認証用データ２を生成する。

Ｓ２１８において、認証処理工程の一部の送信工程として、送信部２１２は、認証用データ２生成部２９５により生成された認証用データ２を通信情報４として通信装置１００に送信する。

Ｓ２１９において、認証処理工程の一部の受信工程として、受信部１１１は、通信装置２００から認証用データ２を通信情報４として受信する。

Ｓ２２０において、認証処理工程の一部として、認証用データ２チェック部１９５は、受信部１１１により通信情報４として受信された暗号化されている認証用データ２を一時鍵生成部１８０により生成された一時鍵により暗号処理部１４０を用いて復号する。

Ｓ２２１において、認証処理工程の一部として、認証用データ２チェック部１９５は、復号した認証用データ２のデータが、通信装置１００が通信装置２００に送信した乱数１のすべて或いは一部であるかどうかを確認する。復号した認証用データ２のデータが乱数１のすべて或いは一部であれば、不正の攻撃者との間ではなく、通信装置２００との間で認証処理のための通信がきちっと行なわれていることを意味する。言い換えれば、通信装置１００，２００間での認証処理の他方が成功したことを意味する。

以上により、通信装置１００，２００間での認証処理が終了し、その

後は、通信装置１００，２００間で一時鍵を用いて暗号化されたデータを通信することにより、データの安全性が確保される。

図３は、通信情報１のフレームの一例を示す図である。

図３において、通信情報１は、ヘッダと乱数１データを有している。

図４は、通信情報２のフレームの一例を示す図である。

図４において、通信情報２は、ヘッダと乱数２データと装置固有番号（装置固有Ｎｏ.）とプロファイル数（Ｐｒｏｆｉｌｅ数）と各プロファイルを識別するプロファイル識別子としてのＰｒｏｆｉｌｅ１，・・・Ｐｒｏｆｉｌｅ　ｎと、各プロファイル識別子に対応するアルゴリズム識別子（アルゴリズムＩＤ）と暗号鍵識別子（鍵ＩＤ）とを有している。図４では、各プロファイル識別子と各プロファイル識別子に対応するアルゴリズム識別子と暗号鍵識別子とは、対応関係がわかるようにデータが構成されている。

図５は、通信情報３のフレームの一例を示す図である。

図５において、通信情報３は、ヘッダと選択された所定のプロファイルを識別する所定のプロファイル識別子としてのＰｒｏｆｉｌｅ　ｋと、所定のプロファイル識別子に対応するアルゴリズム識別子（アルゴリズムＩＤ）と暗号鍵識別子（鍵ＩＤ）と認証用データ１とを有している。図５では、所定のプロファイル識別子と所定のプロファイル識別子に対応するアルゴリズム識別子と暗号鍵識別子とは、対応関係がわかるようにデータが構成されている。

図６は、通信情報４のフレームの一例を示す図である。

図６において、通信情報４は、ヘッダと認証用データ２とを有している。

図７は、通信装置２００側に搭載されているアルゴリズム識別子と暗号鍵識別子とアルゴリズムと個別鍵とを示す図である。

図７において、通信装置２００側では、記憶部２２０に、プロファイルｘｘのアルゴリズム識別子（ＩＤ）と暗号鍵識別子（ＩＤ）とアルゴリズム識別子に対応するアルゴリズムｘと暗号鍵識別子に対応する個別鍵ｘと、プロファイルｙｙのアルゴリズム識別子と暗号鍵識別子とアルゴリズム識別子に対応するアルゴリズムｙと暗号鍵識別子に対応する個別鍵ｙと、・・・プロファイルｚｚのアルゴリズム識別子と暗号鍵識別子とアルゴリズム識別子に対応するアルゴリズムｚと暗号鍵識別子に対応する個別鍵ｚとが記憶されている。すなわち、通信装置２００に搭載（実装）されている。

図８は、通信装置１００側に搭載されているアルゴリズム識別子と暗号鍵識別子とアルゴリズムとを示す図である。

図８において、通信装置１００側では、記憶部１２０に、プロファイルａａのアルゴリズム識別子（ＩＤ）と暗号鍵識別子（ＩＤ）とアルゴリズム識別子に対応するアルゴリズム１と、プロファイルｂｂのアルゴリズム識別子と暗号鍵識別子とアルゴリズム識別子に対応するアルゴリズム２と、・・・プロファイルｃｃのアルゴリズム識別子と暗号鍵識別子とアルゴリズム識別子に対応するアルゴリズムｎとが記憶されている。すなわち、通信装置１００に搭載（実装）されている。

以上のように、認証処理部２９６は、上記受信部２１１により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置となる通信装置１００との間で認証処理をおこなう。すなわち、認証処理部２９６は、上記受信部２１１により受信された所定のアルゴリズム識別子に対応するアルゴリズムと上記受信部により受信された所定の暗号鍵識別子に対応する暗号鍵とを用いて認証処理用暗号鍵となる一時鍵を生成し、生成された認証処理用暗号鍵となる一時鍵を用いて上記認証装置となる通信装置１００との間で認証処理をおこなう。言い

換えれば、上記認証処理部２９６は、上記受信部２１１により受信された所定のプロファイルとして組となる所定のアルゴリズム識別子に対応するアルゴリズムと所定の暗号鍵識別子に対応する暗号鍵とを用いて上記認証処理用暗号鍵となる一時鍵を生成し、生成された認証処理用暗号鍵となる一時鍵を用いて上記認証装置との間で認証処理をおこなう。

一方、認証処理部１９６は、上記送信部１１２により送信される所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記被認証装置となる通信装置２００との間で認証処理をおこなう。すなわち、認証処理部１９６は、上記送信部１１２により送信される所定のアルゴリズム識別子に対応するアルゴリズムと上記送信部１１２により送信された所定の暗号鍵識別子に対応する暗号鍵とを用いて認証処理用暗号鍵となる一時鍵を生成し、生成された認証処理用暗号鍵となる一時鍵を用いて上記被認証装置となる通信装置２００との間で認証処理をおこなう。言い換えれば、上記認証処理部１９６は、上記送信部１１２により送信される所定のプロファイル識別子により識別される所定のプロファイルが組とする所定のアルゴリズム識別子に対応するアルゴリズムと所定の暗号鍵識別子に対応する暗号鍵とを用いて上記認証処理用暗号鍵となる一時鍵を生成し、生成された認証処理用暗号鍵となる一時鍵を用いて上記被認証装置との間で認証処理をおこなう。

ここで、制御部１３０は、通信装置１００の各部を制御する。また、制御部２３０は、通信装置２００の各部を制御する。また、記憶部１２０は、通信装置１００の各部で行なわれる処理中に生じるデータを記憶する。また、記憶部２２０は、通信装置２００の各部で行なわれる処理中に生じるデータを記憶する。

例えば、一例として、ＥＴＣ、ドライブスルー等において、通信装置１００が、店舗側の路側機として、通信装置２００が、自動車側の車載

機として構成される場合に、以上のステップを概括すると以下のようになる。

まず、店舗側の路側機は、車載機に対して、車載機が保持している鍵情報（鍵識別子、アルゴリズム識別子）を要求する。

そして、車載機は、自身が保持している鍵に関する全情報を路側機に送信する。

次に、路側機は、受け取った鍵情報の中から、自身が保持しているアルゴリズム識別子と鍵識別子とが一致しているものを選択し、車載機に選択したアルゴリズム識別子と鍵識別子とを知らせる。

以降、路側機及び車載機は、お互いに共通に保持していたアルゴリズム識別子と鍵識別子とに対応する共通鍵を用いて認証及び鍵共有を実施する。

以上のように、本実施の形態１は、暗号通信に用いるアルゴリズムを複数に対応させるもので、１つのアルゴリズムが解読等で使用できなくなっても他のアルゴリズムを使用することで、引き続きシステムを運用可能とし、アルゴリズム解読等によるセキュリティ低下というリスクを軽減させることができる。また、複数のアルゴリズムを使いこなすことにより、同一のアルゴリズムを使用する回数が減ることにより、不正の攻撃者による解読の機会を減らし、セキュリティを向上させることができる。さらに、新たに考案されたアルゴリズムを通信装置に搭載することができることから、新たに考案されたアルゴリズムの適用をも容易にすることができる。通信装置１００，２００のうち、少なくとも一方において、アルゴリズム識別子と鍵識別子との組が複数存在すれば、選択肢ができることになり、上記効果が得られる。なお、この実施形態１では、装置１００，２００の少なくとも一方に複数のアルゴリズム識別子と暗号鍵識別子との組が複数存在すればよいとした。しかし、この発明

はアルゴリズム識別子と暗号鍵識別子の少なくとも１組が一致すれば認証が行えるため、必ずしも装置１００，２００の少なくとも一方に複数組存在する必要はなく各装置に１組だけが存在していてもよい。また、各装置に１組だけしか存在していてもよいことから、一つの暗号アルゴリズムしか使用しない従来例にもこの発明による認証方法を適用可能である。

実施の形態２.

図９は、実施の形態２における認証システムの構成を示す図である。

図９において、通信装置２００における認証処理部２９６は、図１の構成に対し、さらに、認証用データ１生成部２９１を有している。その他の各構成は、図１と同様である。

図１０は、実施の形態２における認証方法を示すフローチャート図である。

図１０において、図２のＳ２１５，Ｓ２１６がＳ１０１５、Ｓ１０１６に代わった以外は、図２と同様である。

Ｓ１０１５において、認証処理工程の一部として、認証用データ１生成部２９１は、乱数２のすべて或いは一部を暗号処理部２４０により一時鍵生成部２８０により生成された一時鍵で暗号化することにより認証用データ１を生成する。

Ｓ１０１６において、認証処理工程の一部として、認証用データ１チェック部２９０は、通信情報３として受信部２１１により受信された暗号化されたままの認証用データ１と認証用データ１生成部２９１により生成された認証用データ１とが一致するかどうかを確認する。一致すれば、不正の攻撃者との間ではなく、通信装置１００との間で認証処理のための通信がきちっと行なわれていることを意味する。言い換えれば、

通信装置１００，２００間での認証処理の一方が成功したことを意味する。

以上のように構成しても実施の形態１と同様の効果を得ることができる。

実施の形態３.

実施の形態３における各構成は、図１と同様である。

図１１は、実施の形態３における認証方法を示すフローチャート図である。

図１１では、図２のＳ２０２，Ｓ２０３が無いこと以外は、図２と同様である。

実施の形態３では、認証側となる通信装置１００が通信装置２００に通信情報１を送信しなくても通信装置２００から通信装置１００へ通信情報２を送信する構成となっている。かかるステップを省略することにより、より高速に認証フローを実施することができる。

以上のように構成しても実施の形態１と同様の効果を得ることができる。

実施の形態４.

実施の形態４における各構成は、図１と同様である。

図１２は、実施の形態４における認証方法を示すフローチャート図である。

図１２では、図２のＳ２０５、Ｓ２０６，Ｓ２０７，Ｓ２１１，Ｓ２１２が、Ｓ１２０５，Ｓ１２０６，Ｓ１２０７，Ｓ１２１１，Ｓ１２１２に代わった以外は、図２と同様である。

実施の形態４では、記憶部２２０は、さらに、記憶された少なくとも

１つのアルゴリズム識別子に対応する少なくとも１つのアルゴリズムを１つのセットとした上記セットを示すバージョンを識別するバージョン識別子（ＩＤ）を記憶する。

同様に、記憶部１２０は、さらに、記憶された少なくとも１つのアルゴリズム識別子に対応する少なくとも１つのアルゴリズムを１つのセットとして、上記セットのバージョンを識別するバージョン識別子（ＩＤ）を記憶する。

例えば、バージョン識別子としてのバージョン１が識別するバージョンは、アルゴリズムとしてＤＥＳだけをサポートする。バージョン２が識別するバージョンは、アルゴリズムとしてＤＥＳ、ＭＩＳＴＹをサポートする。バージョン３が識別するバージョンは、アルゴリズムとしてＤＥＳ、ＭＩＳＴＹ、Ｃａｍｅｌｌｉａ、ＡＥＳをサポートする。

Ｓ１２０５において、送信工程（第１の送信工程）として、送信部２１２は、上記記憶部２２０により記憶された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子と装置固有番号と、乱数生成部２５０により生成された乱数２と、さらに、記憶部２２０により記憶されたバージョン識別子とを通信情報２－１として認証装置である通信装置１００に送信する。

Ｓ１２０６において、受信工程（第１の受信工程）として、受信部１１１は、被認証装置となる通信装置２００から、乱数２と装置固有番号と組数分のプロファイル数とプロファイル数分の少なくとも１つのプロファイル識別子と少なくとも１つのプロファイル識別子の各プロファイル識別子に対応した少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子と、さらに、所定のバージョン識別子とを有する通信情報２－１を受信する。

Ｓ１２０７において、選択工程として、選択部１６０は、上記受信部

１１１により受信された所定のバージョン識別子が識別するバージョンが示すセットの中に上記記憶部１２０により記憶された少なくとも１つのアルゴリズムが存在する場合に、上記受信部１１１により受信された所定のバージョン識別子が識別するバージョンが示すセットの中から上記記憶部１２０により記憶されるアルゴリズムに対応する所定のアルゴリズム識別子を選択する。例えば、通信装置２００が古いバージョンしか対応していない場合に、古いバージョンが示すアルゴリズムがすべてセキュリティ上問題がある場合、選択せずに以降の認証処理を終了させることもできる。一方、１つでも認証処理に使用可能なアルゴリズムがあれば、その使用可能なアルゴリズムを使って、以降の認証処理を行なわせることができる。バージョン識別子を用いることで、バージョン識別子から通信装置２００が使用可能なアルゴリズムを搭載しているかどうかを判断することができる。

Ｓ１２１１において、送信工程（第２の送信工程）として、送信部１１２は、上記選択部１６０により選択された所定のアルゴリズム識別子と認証用データ１生成部１９０により生成された認証用データ１とを通信情報３－１として上記被認証装置となる通信装置２００に送信する。

Ｓ１２１２において、受信工程として、受信部２１１は、上記認証装置となる通信装置１００から上記送信部２１２により送信されたバージョン識別子が識別するバージョンが示すセットとなる上記記憶部２２０により記憶された少なくとも１つのアルゴリズムの中から選択された所定のアルゴリズムに対応する所定のアルゴリズム識別子と認証用データ１とを通信情報３－１として受信する。

以降、認証処理部２９６は、上記受信部２１１により受信された所定のアルゴリズム識別子に対応する所定のアルゴリズムと上記所定のアルゴリズム識別子と組となる所定の暗号鍵識別子に対応する所定の暗号鍵

とを用いて上記認証処理用暗号鍵を生成し、生成された認証処理用暗号鍵を用いて上記認証装置との間で認証処理をおこなう。

同様に、認証処理部１９６は、上記送信部１１２により送信される所定のアルゴリズム識別子に対応するアルゴリズムと上記所定のアルゴリズム識別子と組となる所定の暗号鍵識別子に対応する暗号鍵とを用いて上記認証処理用暗号鍵を生成し、生成された認証処理用暗号鍵を用いて上記被認証装置との間で認証処理をおこなう。

以上のように構成することで、実施の形態１の効果に加え、セキュリティ上問題がある古いバージョンを排除することもできる。

ここで、実施の形態４では、選択部１６０が、所定のアルゴリズム識別子を選択しているが、さらに、選択した所定のアルゴリズム識別子に対応する所定の暗号鍵識別子を選択してもかまわない。かかる場合、図１２におけるＳ１２１１，Ｓ１２１２は、図２におけるＳ２１１，Ｓ２１２のままで構わない。

実施の形態５.

実施の形態５における各構成は、図１と同様である。

図１３は、実施の形態５における認証方法を示すフローチャート図である。

図１３では、図２のＳ２０５、Ｓ２０６、Ｓ２０７が、Ｓ１３０５、Ｓ１３０６、Ｓ１３０７、Ｓ１３０８、Ｓ１３０９、Ｓ１３１０、Ｓ１３１１、Ｓ１３０７に代わった以外は、図２と同様である。

実施の形態５では、実施の形態４と同様に、記憶部２２０は、さらに、記憶された少なくとも１つのアルゴリズム識別子に対応する少なくとも１つのアルゴリズムを１つのセットとした上記セットを示すバージョンを識別するバージョン識別子（ＩＤ）を記憶する。

同様に、記憶部１２０は、さらに、記憶された少なくとも１つのアルゴリズム識別子に対応する少なくとも１つのアルゴリズムを１つのセットとして、上記セットのバージョンを識別するバージョン識別子（ＩＤ）を記憶する。

Ｓ１３０５において、送信工程として、送信部２１２は、上記記憶部２２０により記憶された装置固有番号と、乱数生成部２５０により生成された乱数２と、さらに、記憶部２２０により記憶されたバージョン識別子とを通信情報２－２として認証装置である通信装置２００に送信する。

Ｓ１３０６において、受信工程（第１の受信工程）として、受信部１１１は、被認証装置となる通信装置２００から、乱数２と装置固有番号と所定のバージョン識別子とを有する通信情報２－２を受信する。

Ｓ１３０７において、選択工程として、選択部１６０は、上記受信部１１１により受信された所定のバージョン識別子が、記憶部１２０に記憶されたバージョン識別子と一致する場合は、そのバージョン識別子を選択し、一致しない場合には、所定のバージョン識別子が示すセットの中に上記記憶部１２０により記憶された少なくとも１つのアルゴリズムが存在する場合に、上記記憶部１２０により記憶された少なくとも１つのアルゴリズムが存在するセットを示すバージョンのバージョン識別子を選択する。例えば、記憶部１２０に記憶されたバージョン識別子の方が、上記受信部１１１により受信された所定のバージョン識別子より最新バージョンのバージョン識別子である場合に、通信装置１００，２００に共通するように古いバージョンとなる上記受信部１１１により受信された所定のバージョン識別子を選択する。通信装置１００，２００に共通する古いバージョンを選択することにより以降の認証処理を続行させ、鍵共有をおこなうことができる。

Ｓ１３０８において、送信工程として、送信部１１２は、選択部１６０により選択されたバージョン識別子（ＩＤ）を通信情報２－３として通信装置２００に送信する。

Ｓ１３０９において、受信工程として、受信部２１１は、通信装置１００よりバージョン識別子（ＩＤ）を通信情報２－３として受信する。

Ｓ１３１０において、送信工程として、送信部２１２は、上記記憶部２２０により記憶された少なくとも１つのプロファイル識別子と各プロファイル識別子が表すプロファイルに組とされるアルゴリズム識別子と暗号鍵識別子と組数分のプロファイル数とを通信情報２－４として認証装置である通信装置２００に送信する。

Ｓ１３１１において、受信工程として、受信部１１１は、被認証装置となる通信装置２００から、少なくとも１つのプロファイル識別子と各プロファイル識別子が表すプロファイルに組とされるアルゴリズム識別子と暗号鍵識別子と組数分のプロファイル数とを通信情報２－４として受信する。ここで、乱数２と装置固有番号とを通信情報２－２に含めているが、通信情報２－４に含めていても構わない。

Ｓ１３１２において、選択工程として、選択部１６０は、上記受信部１１１により受信された少なくとも１つのプロファイル識別子の中に上記記憶部１２０により記憶された少なくとも１つのプロファイル識別子が存在する場合に、上記受信部１１１により受信された少なくとも１つのプロファイル識別子の中から上記記憶部１２０により記憶される所定のプロファイル識別子を選択する。所定のプロファイル識別子を選択することで、所定のプロファイル識別子が示すプロファイルに組みする所定のアルゴリズム識別子と所定の暗号鍵識別子とが選択される。

以上のように、実施の形態５では、実施の形態４と比較し、まず、バージョン選択という工程を別に行なう形態である。以上のように構成し

ても実施の形態４と同様の効果を得ることができる。そして、実施の形態１の効果に加え、セキュリティ上問題があるアルゴリズムを排除することもできる。

以上のように、上記実施の形態における認証方法は、複数のアルゴリズム識別子と複数の暗号鍵識別子とを記憶する被認証装置から記憶された複数のアルゴリズム識別子と複数の暗号鍵識別子とを認証装置に送信する第１の送信工程と、少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを記憶する認証装置が、上記第１の送信工程により被認証装置から送信された複数のアルゴリズム識別子と複数の暗号鍵識別子とを受信する第１の受信工程と、上記第１の受信工程により受信された複数のアルゴリズム識別子と複数の暗号鍵識別子との中に上記認証装置により記憶された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とが存在する場合に、上記認証装置が上記受信工程により受信された複数のアルゴリズム識別子と複数の暗号鍵識別子との中から上記認証装置により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択する選択工程と、上記選択工程により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置から上記被認証装置に送信する第２の送信工程と、上記被認証装置が上記認証装置から上記第２の送信工程により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する第２の受信工程と、上記第２の受信工程により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置と上記被認証装置との間で認証処理をおこなう認証処理工程とを備えている。

或いは、少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを記憶する被認証装置から記憶された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを認証装置に送信

する第１の送信工程と、複数のアルゴリズム識別子と複数の暗号鍵識別子とを記憶する認証装置が、上記第１の送信工程により被認証装置から送信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを受信する第１の受信工程と、上記第１の受信工程により受信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子との中に上記認証装置により記憶された複数のアルゴリズム識別子の少なくとも１つと複数の暗号鍵識別子の少なくとも１つとが存在する場合に、上記認証装置が上記受信工程により受信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子との中から上記認証装置により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択する選択工程と、上記選択工程により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置から上記被認証装置に送信する第２の送信工程と、上記被認証装置が上記認証装置から上記第２の送信工程により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する第２の受信工程と、上記第２の受信工程により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置と上記被認証装置との間で認証処理をおこなう認証処理工程とを備えている。

以上の説明において、各実施の形態の説明において「～部」として説明したものは、一部或いはすべてコンピュータで動作可能なプログラムにより構成することができる。これらのプログラムは、例えば、Ｃ言語により作成することができる。或いは、ＨＴＭＬやＳＧＭＬやＸＭＬを用いても構わない。

図１４は、ハードウェア構成図である。

以上の説明において、各実施の形態の説明において「～部」として説明したものを、一部或いはすべてコンピュータで動作可能なプログラム

により構成する場合、図１４に示すように、通信装置１００，２００は、プログラムを実行するＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）３７を備えている。ＣＰＵ３７は、内蔵された、或いはバス３８を介してＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）４０（記憶装置、記憶部の一例である）、外部と通信可能な通信ポート４４に接続されている。また、図１４に示すように、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）３９、磁気ディスク装置４６等の記憶装置に接続されていても構わない。

プログラムにより構成する場合、図１４におけるプログラム群４９には、各実施の形態の説明において「～部」として説明したものにより実行されるプログラムが記憶されている。プログラム群４９は、上記記憶装置に記憶されている。プログラム群４９は、ＣＰＵ３７、ＯＳ４７等により実行される。記憶装置は、各処理の結果を記憶する。

また、各実施の形態の説明において「～部」として説明したものは、ＲＯＭ３９に記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェア或いは、ハードウェア或いは、ソフトウェアとハードウェアとファームウェアとの組み合わせで実施されても構わない。

また、上記各実施の形態を実施させるプログラムは、ＦＤ（Ｆｌｅｘｉｂｌｅ Ｄｉｓｋ）、光ディスク、ＣＤ（コンパクトディスク）、ＭＤ（ミニディスク）、ＤＶＤ（Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｋ）等のその他の記録媒体による記録装置を用いて記憶されても構わない。係る場合には、図１４に示すように、ＦＤＤ（Ｆｌｅｘｉｂｌｅ Ｄｉｓｋ Ｄｒｉｖｅ）４５、コンパクトディスク装置（ＣＤＤ）８６等を備える。

産業上の利用可能性

このような通信装置１００，２００は、ＥＴＣ、ドライブスルー等における店舗側の路側機と自動車側の車載機に限らず、携帯電話等の移動体通信装置間、有線の通信装置間、或いは基地局を経由した有線と無線の通信装置間等における認証装置、被認証装置として、使用することができる。

本発明によれば、異なるアルゴリズムを実装している装置間でも認証及び鍵共有が行なえるようにすることができ、１つのアルゴリズムが解読等により使用できなくなっても引き続きシステム及び装置を運用可能とすることができる。

また、アルゴリズムの解読等によるセキュリティ低下というリスクを軽減することができる。

また、盗聴等による不正な解読等の機会を減らし、セキュリティを向上させることができる。

請求の範囲

1．少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを記憶する記憶部と、

上記記憶部により記憶された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを認証装置に送信する送信部と、

上記認証装置から上記送信部により送信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子との中から選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する受信部と、

上記受信部により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子に基づいて上記認証装置との間で認証処理をおこなう認証処理部と

を備えたことを特徴とする被認証装置。

2．上記記憶部は、1つのアルゴリズム識別子と1つの暗号鍵識別子とを1組のプロファイルとして、少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを記憶し、

上記送信部は、上記記憶部により1つのアルゴリズム識別子と1つの暗号鍵識別子とを1組のプロファイルとして記憶された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを認証装置に送信し、

上記受信部は、上記認証装置から上記送信部により送信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子との中から所定のプロファイルとして組となる上記所定のアルゴリズム識別子と上記所定の暗号鍵識別子とを受信し、

上記認証処理部は、上記受信部により受信された所定のプロファイル

として組となる所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置との間で認証処理をおこなうことを特徴とする請求項１記載の被認証装置。

３．上記記憶部は、さらに、記憶された少なくとも１つのアルゴリズム識別子に対応する少なくとも１つのアルゴリズムを１つのセットとした上記セットを示すバージョンを識別するバージョン識別子を記憶し、

上記送信部は、上記記憶部により記憶されたバージョン識別子を認証装置に送信し、

上記受信部は、上記認証装置から上記送信部により送信されたバージョン識別子が識別するバージョンが示すセットとなる少なくとも１つのアルゴリズムの中の所定のアルゴリズムに対応する上記所定のアルゴリズム識別子を受信し、

上記認証処理部は、上記受信部により受信された所定のアルゴリズム識別子と上記所定のアルゴリズム識別子と組となる所定の暗号鍵識別子とに基づいて上記認証装置との間で認証処理をおこなうことを特徴とする請求項２記載の被認証装置。

４．少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを記憶する記憶部と、

被認証装置から少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを受信する受信部と、

上記受信部により受信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子との中に上記記憶部により記憶された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とが存在する場合に、上記受信部により受信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子との中から上記記憶部

により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択する選択部と、

上記選択部により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記被認証装置に送信する送信部と、

上記送信部により送信される所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記被認証装置との間で認証処理をおこなう認証処理部と

を備えたことを特徴とする認証装置。

5．上記記憶部は、少なくとも１つのアルゴリズム識別子の１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子の１つの暗号鍵識別子とを組とする少なくとも１つのプロファイルを識別する少なくとも１つのプロファイル識別子を記憶し、

上記受信部は、さらに、上記被認証装置から少なくとも１つのプロファイル識別子を受信し、

上記選択部は、上記受信部により受信された少なくとも１つのプロファイル識別子の中に上記記憶部により記憶された少なくとも１つのプロファイル識別子が存在する場合に、上記受信部により受信された少なくとも１つのプロファイル識別子の中から上記記憶部により記憶される所定のプロファイル識別子を選択し、

上記送信部は、上記選択部により選択された所定のプロファイル識別子を上記被認証装置に送信し、

上記認証処理部は、上記送信部により送信される所定のプロファイル識別子により識別される所定のプロファイルが組とする上記所定のアルゴリズム識別子と上記所定の暗号鍵識別子とに基づいて上記被認証装置との間で認証処理をおこなうことを特徴とする請求項４記載の認証装置。

6．上記記憶部は、さらに、記憶された少なくとも１つのアルゴリズム識別子に対応する少なくとも１つのアルゴリズムを１つのセットとして、上記セットのバージョンを識別するバージョン識別子を記憶し、

上記受信部は、さらに、上記被認証装置から所定のバージョン識別子を受信し、

上記選択部は、上記受信部により受信された所定のバージョン識別子が識別するバージョンが示すセットの中の１つのアルゴリズムに対応する上記所定のアルゴリズム識別子を選択し、

上記送信部は、上記選択部により選択された所定のアルゴリズム識別子を上記被認証装置に送信し、

上記認証処理部は、上記送信部により送信される所定のアルゴリズム識別子と上記所定のアルゴリズム識別子と組となる所定の暗号鍵識別子とに基づいて上記被認証装置との間で認証処理をおこなうことを特徴とする請求項５記載の認証装置。

7．複数のアルゴリズム識別子と複数の暗号鍵識別子とを記憶する被認証装置から記憶された複数のアルゴリズム識別子と複数の暗号鍵識別子とを認証装置に送信する第１の送信工程と、

少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを記憶する認証装置が、上記第１の送信工程により被認証装置から送信された複数のアルゴリズム識別子と複数の暗号鍵識別子とを受信する第１の受信工程と、

上記第１の受信工程により受信された複数のアルゴリズム識別子と複数の暗号鍵識別子との中に上記認証装置により記憶された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とが存在する場合に、上記認証装置が上記受信工程により受信された複数のアルゴリズム識別子と複数の暗号鍵識別子との中から上記認証装置により記憶さ

れる所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択する選択工程と、

上記選択工程により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置から上記被認証装置に送信する第２の送信工程と、

上記被認証装置が上記認証装置から上記第２の送信工程により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する第２の受信工程と、

上記第２の受信工程により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置と上記被認証装置との間で認証処理をおこなう認証処理工程とを備えたことを特徴とする認証方法。

８．少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを記憶する被認証装置から記憶された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを認証装置に送信する第１の送信工程と、

複数のアルゴリズム識別子と複数の暗号鍵識別子とを記憶する認証装置が、上記第１の送信工程により被認証装置から送信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを受信する第１の受信工程と、

上記第１の受信工程により受信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子との中に上記認証装置により記憶された複数のアルゴリズム識別子の少なくとも１つと複数の暗号鍵識別子の少なくとも１つとが存在する場合に、上記認証装置が上記受信工程により受信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子との中から上記認証装置により記憶される所定のア

ルゴリズム識別子と所定の暗号鍵識別子とを選択する選択工程と、

上記選択工程により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置から上記被認証装置に送信する第２の送信工程と、

上記被認証装置が上記認証装置から上記第２の送信工程により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する第２の受信工程と、

上記第２の受信工程により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置と上記被認証装置との間で認証処理をおこなう認証処理工程とを備えたことを特徴とする認証方法。

９．複数のアルゴリズム識別子と複数の暗号鍵識別子とを記憶する被認証装置から記憶された複数のアルゴリズム識別子と複数の暗号鍵識別子とを認証装置に送信し、

少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを記憶する認証装置が、被認証装置から送信された複数のアルゴリズム識別子と複数の暗号鍵識別子とを受信し、

受信された複数のアルゴリズム識別子と複数の暗号鍵識別子との中に上記認証装置により記憶された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とが存在する場合に、上記認証装置が受信された複数のアルゴリズム識別子と複数の暗号鍵識別子との中から上記認証装置により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択し、

選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置から上記被認証装置に送信し、

上記被認証装置が上記認証装置から送信された所定のアルゴリズム識

別子と所定の暗号鍵識別子とを受信し、

受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置と上記被認証装置との間で認証処理をおこなうことを特徴とする認証方法。

１０．少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを記憶する被認証装置から記憶された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを認証装置に送信し、

複数のアルゴリズム識別子と複数の暗号鍵識別子とを記憶する認証装置が、被認証装置から送信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子とを受信し、

受信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子との中に上記認証装置により記憶された複数のアルゴリズム識別子の少なくとも１つと複数の暗号鍵識別子の少なくとも１つとが存在する場合に、上記認証装置が受信された少なくとも１つのアルゴリズム識別子と少なくとも１つの暗号鍵識別子との中から上記認証装置により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択し、

選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置から上記被認証装置に送信し、

上記被認証装置が上記認証装置から送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信し、

受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置と上記被認証装置との間で認証処理をおこなうことを特徴とする認証方法。

図1

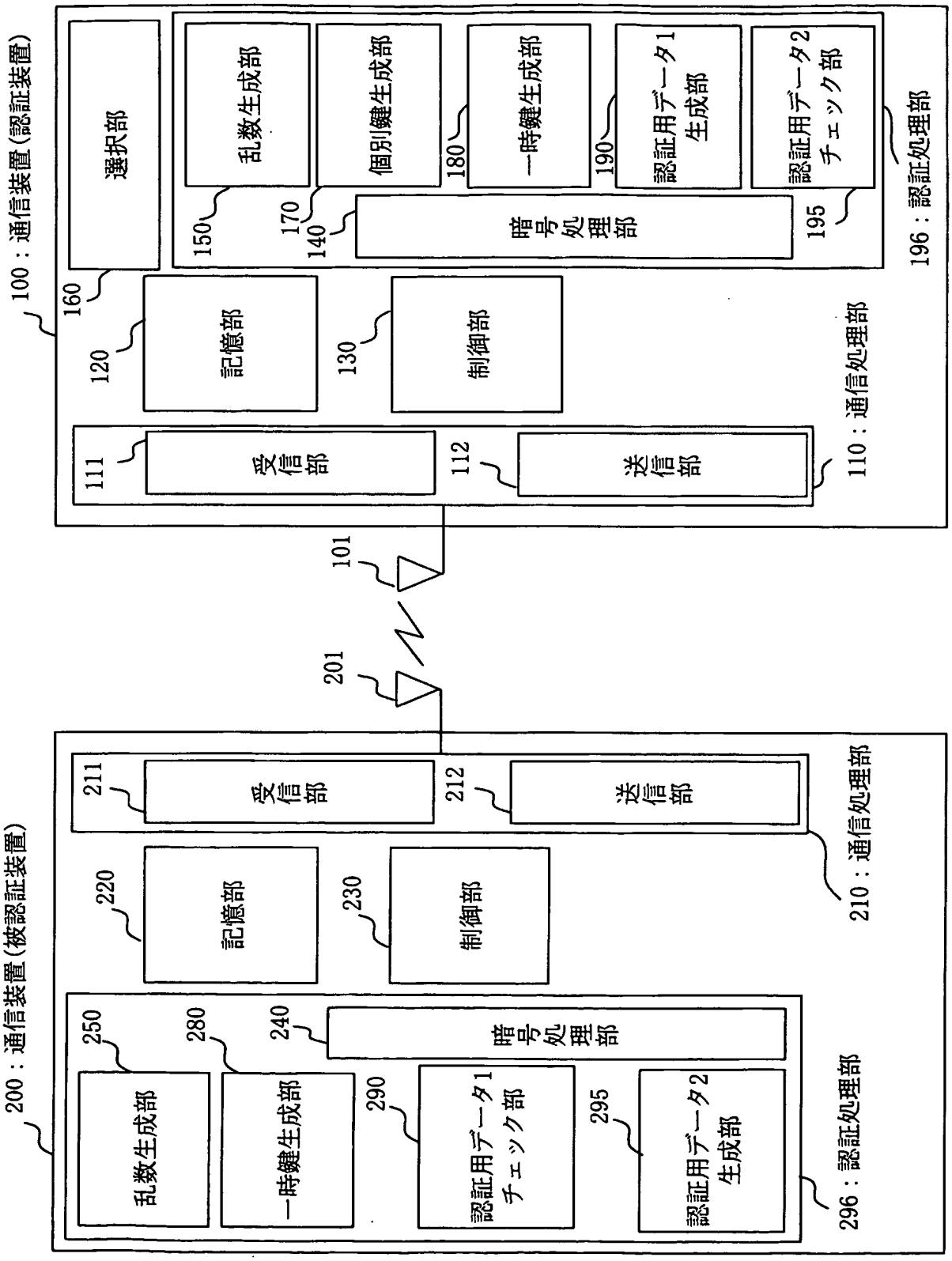

100：通信装置(認証装置)
選択部
160
乱数生成部
150
個別鍵生成部
170
一時鍵生成部
180
認証用データ1生成部
190
認証用データ2チェック部
195
暗号処理部
140
196：認証処理部
記憶部
120
制御部
130
受信部
111
送信部
112
110：通信処理部
101
201
200：通信装置(被認証装置)
211
受信部
212
送信部
210：通信処理部
220
記憶部
230
制御部
250
乱数生成部
280
一時鍵生成部
240
暗号処理部
290
認証用データ1チェック部
295
認証用データ2生成部
296：認証処理部

図2

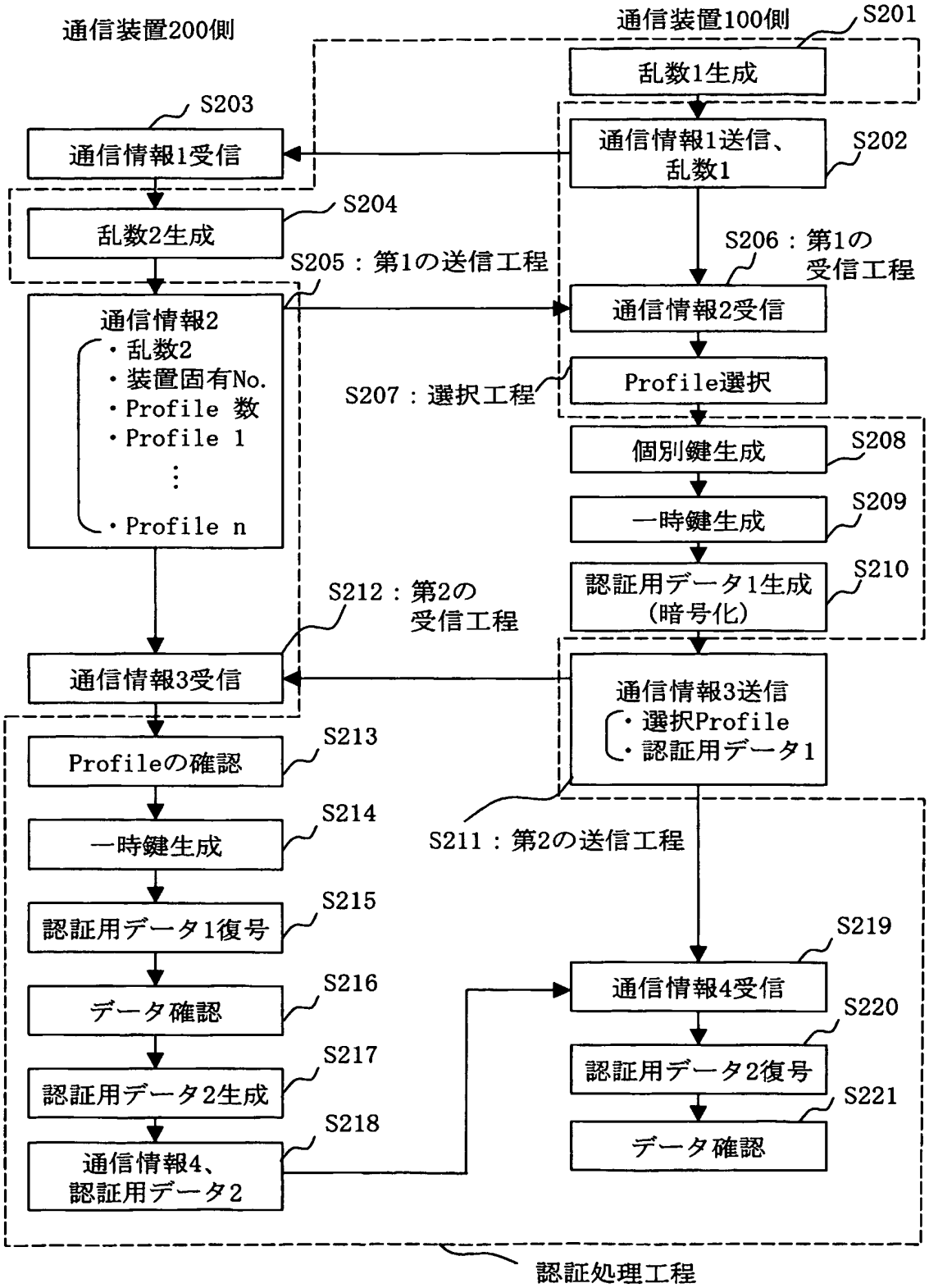

通信装置200側
通信装置100側
S201
乱数1生成
S203
通信情報1受信
通信情報1送信、
乱数1
S202
乱数2生成
S204
S205：第1の送信工程
S206：第1の
受信工程
通信情報2
・乱数2
・装置固有No.
・Profile 数
・Profile 1
・Profile n
通信情報2受信
S207：選択工程
Profile選択
個別鍵生成
S208
一時鍵生成
S209
認証用データ1生成
(暗号化)
S210
S212：第2の
受信工程
通信情報3受信
通信情報3送信
・選択Profile
・認証用データ1
S213
Profileの確認
S214
一時鍵生成
S211：第2の送信工程
S215
認証用データ1復号
S219
通信情報4受信
S216
データ確認
S220
認証用データ2復号
S217
認証用データ2生成
S221
データ確認
S218
通信情報4、
認証用データ2
認証処理工程

図3

通信情報1

ヘッダ
乱数1

図4

通信情報2

ヘッダ		
乱数2		
装置固有No.		
Profile 数		
Profile 1	アルゴリズムID	鍵ID
・ ・ ・	・ ・ ・	・ ・ ・
Profile n	アルゴリズムID	鍵ID

図5

通信情報3

ヘッダ		
Profile k	アルゴリズムID	鍵ID
認証用データ1		

図6

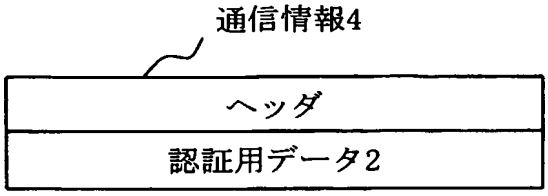

通信情報4
ヘッダ
認証用データ2

図7

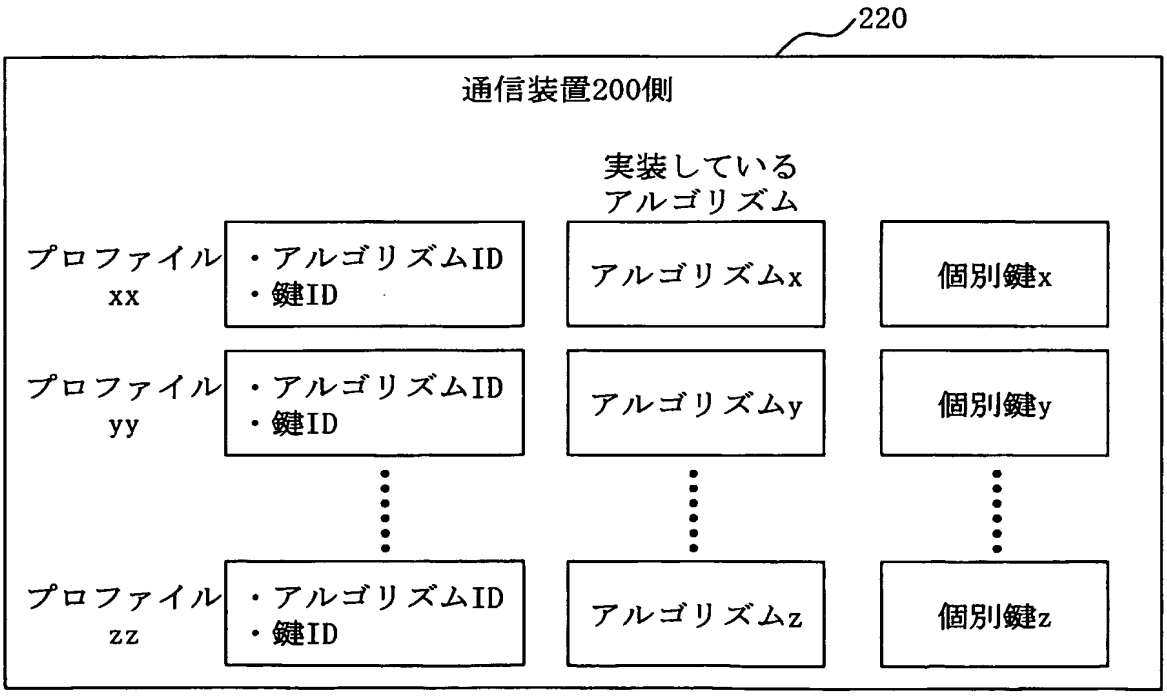

220
通信装置200側
実装している
アルゴリズム
プロファイル
xx
・アルゴリズムID
・鍵ID
アルゴリズムx
個別鍵x
プロファイル
yy
・アルゴリズムID
・鍵ID
アルゴリズムy
個別鍵y
プロファイル
zz
・アルゴリズムID
・鍵ID
アルゴリズムz
個別鍵z

図8

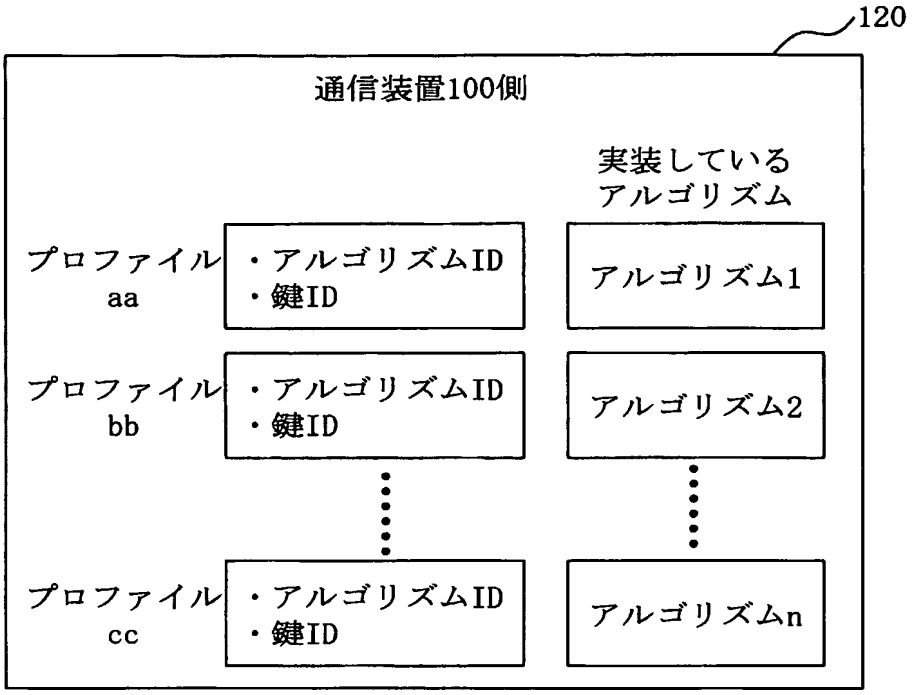

120
通信装置100側
実装している
アルゴリズム
プロファイル
aa
・アルゴリズムID
・鍵ID
アルゴリズム1
プロファイル
bb
・アルゴリズムID
・鍵ID
アルゴリズム2
プロファイル
cc
・アルゴリズムID
・鍵ID
アルゴリズムn

図9

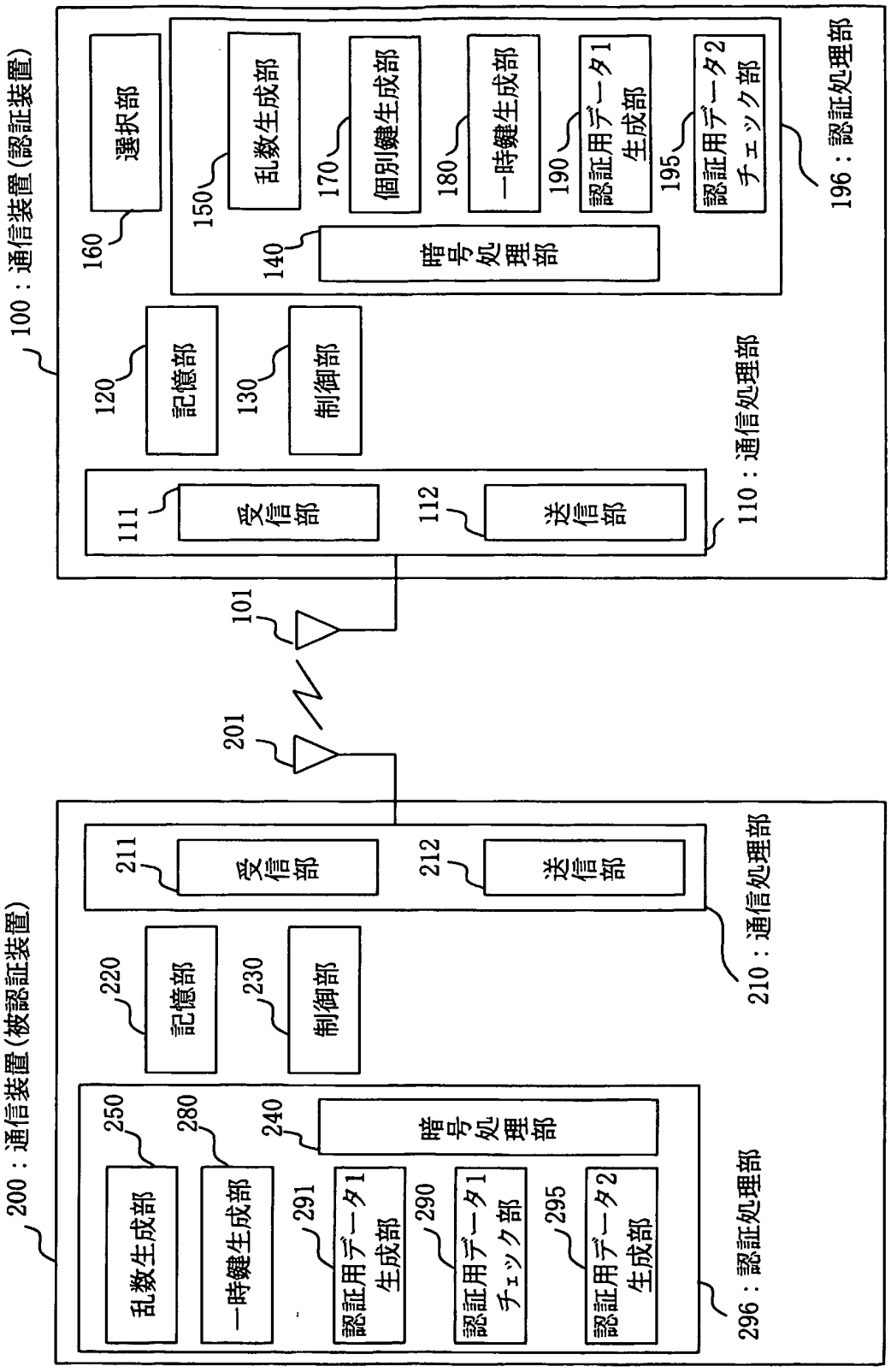

100：通信装置(認証装置)
160
選択部
150
乱数生成部
170
個別鍵生成部
180
一時鍵生成部
190
認証用データ1生成部
195
認証用データ2チェック部
140
暗号処理部
196：認証処理部
120
記憶部
130
制御部
111
受信部
112
送信部
110：通信処理部
101
201
200：通信装置(被認証装置)
211
受信部
212
送信部
210：通信処理部
220
記憶部
230
制御部
250
乱数生成部
280
一時鍵生成部
240
暗号処理部
291
認証用データ1生成部
290
認証用データ1チェック部
295
認証用データ2生成部
296：認証処理部

図10

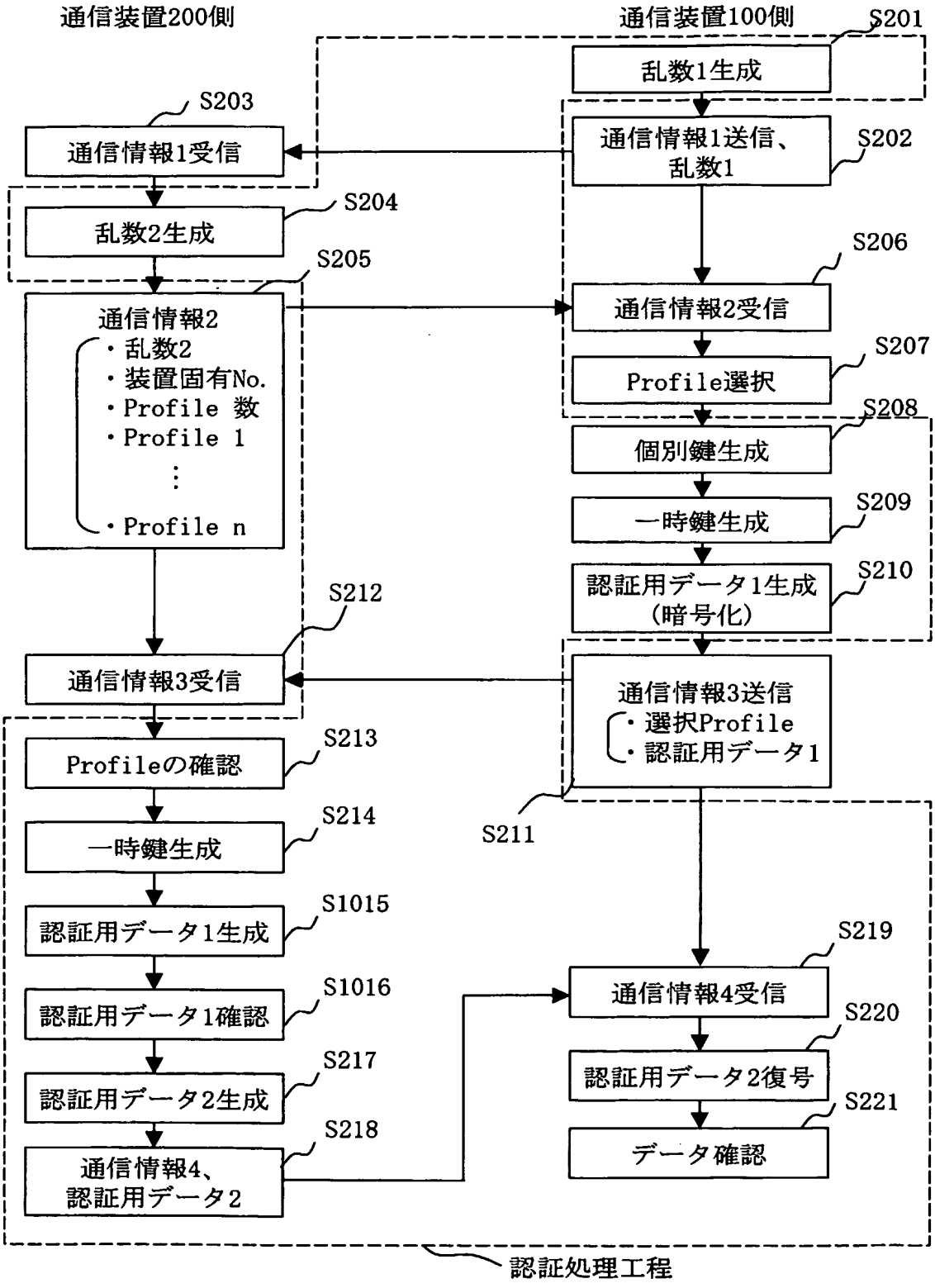

通信装置200側
通信装置100側
S201
乱数1生成
S203
通信情報1受信
通信情報1送信、
乱数1
S202
S204
乱数2生成
S206
S205
通信情報2
・乱数2
・装置固有No.
・Profile 数
・Profile 1
・Profile n
通信情報2受信
S207
Profile選択
S208
個別鍵生成
S209
一時鍵生成
S210
認証用データ1生成
(暗号化)
S212
通信情報3受信
通信情報3送信
・選択Profile
・認証用データ1
S211
S213
Profileの確認
S214
一時鍵生成
S1015
認証用データ1生成
S219
通信情報4受信
S1016
認証用データ1確認
S220
認証用データ2復号
S217
認証用データ2生成
S221
データ確認
S218
通信情報4、
認証用データ2
認証処理工程

図11

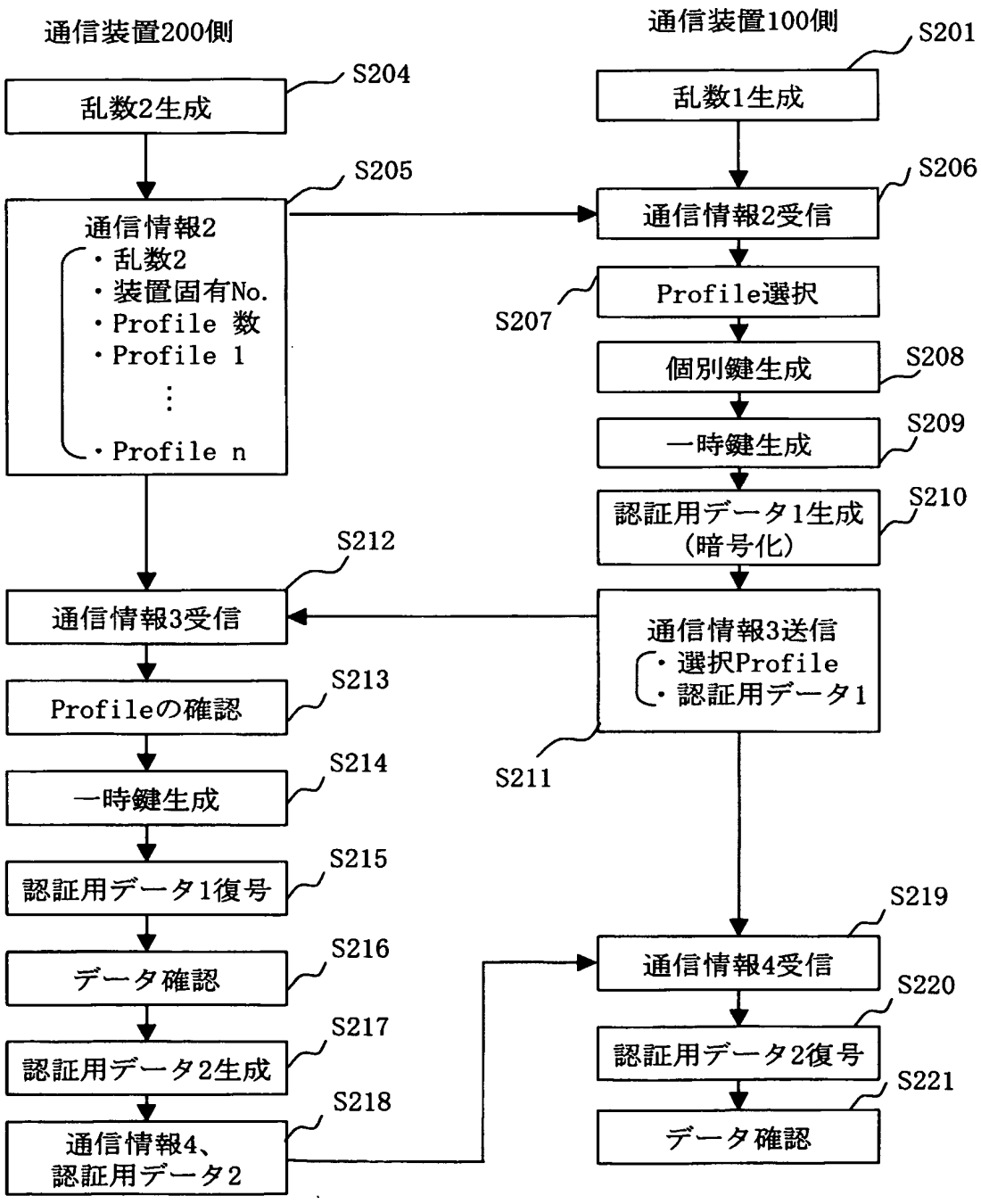
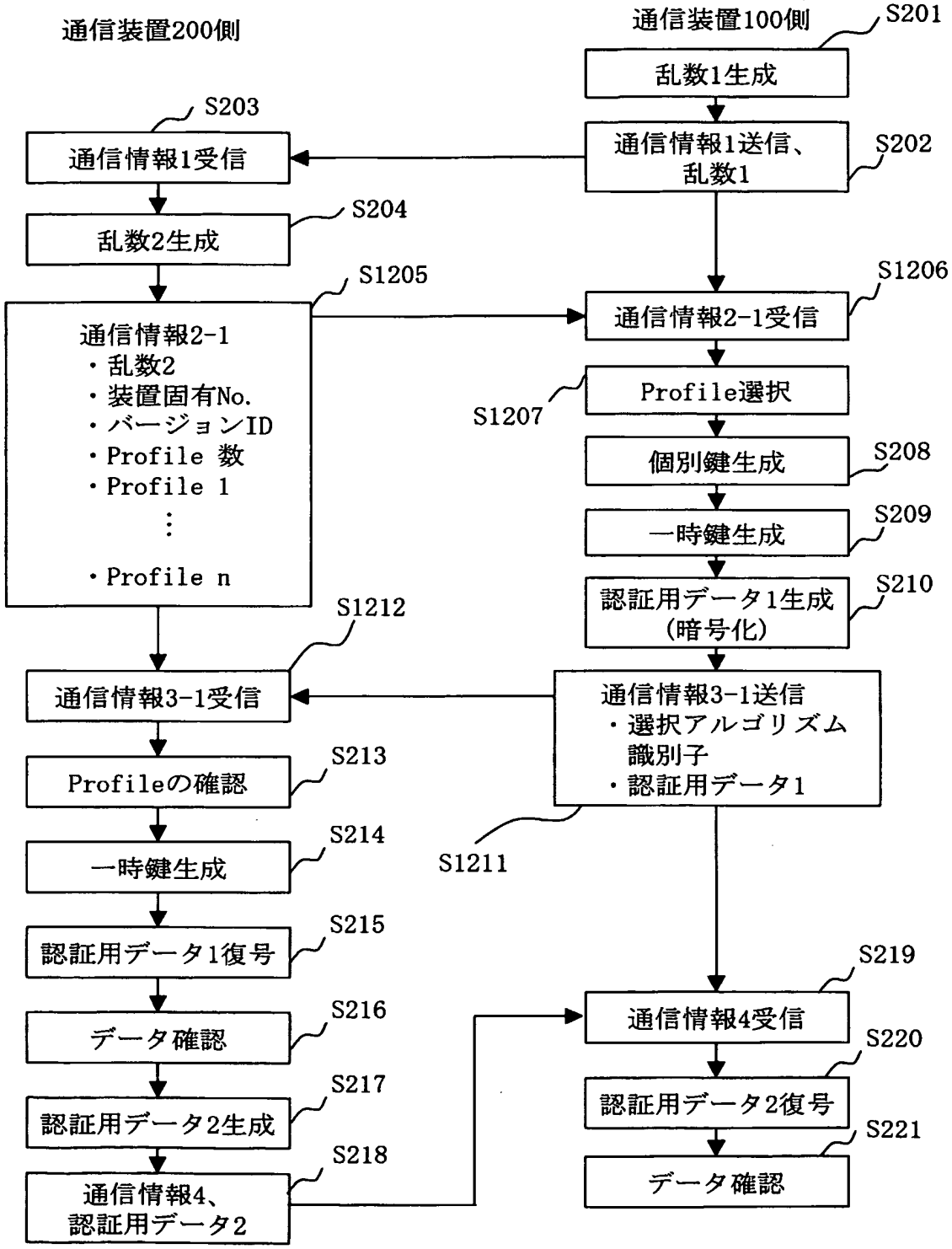

通信装置200側
通信装置100側
S201
乱数1生成
S204
乱数2生成
S205
通信情報2
・乱数2
・装置固有No.
・Profile 数
・Profile 1
・Profile n
S206
通信情報2受信
S207
Profile選択
S208
個別鍵生成
S209
一時鍵生成
S210
認証用データ1生成
(暗号化)
S211
通信情報3送信
・選択Profile
・認証用データ1
S212
通信情報3受信
S213
Profileの確認
S214
一時鍵生成
S215
認証用データ1復号
S216
データ確認
S217
認証用データ2生成
S218
通信情報4、
認証用データ2
S219
通信情報4受信
S220
認証用データ2復号
S221
データ確認

図12


通信装置200側
通信装置100側
S201
乱数1生成
S203
通信情報1受信
通信情報1送信、
乱数1
S202
S204
乱数2生成
S1205
S1206
通信情報2-1
・乱数2
・装置固有No.
・バージョンID
・Profile 数
・Profile 1
・Profile n
通信情報2-1受信
S1207
Profile選択
個別鍵生成
S208
一時鍵生成
S209
認証用データ1生成
(暗号化)
S210
S1212
通信情報3-1受信
通信情報3-1送信
・選択アルゴリズム
識別子
・認証用データ1
S213
Profileの確認
S214
一時鍵生成
S1211
S215
認証用データ1復号
S219
通信情報4受信
S216
データ確認
S220
認証用データ2復号
S217
認証用データ2生成
S221
データ確認
S218
通信情報4、
認証用データ2

10/11

図13

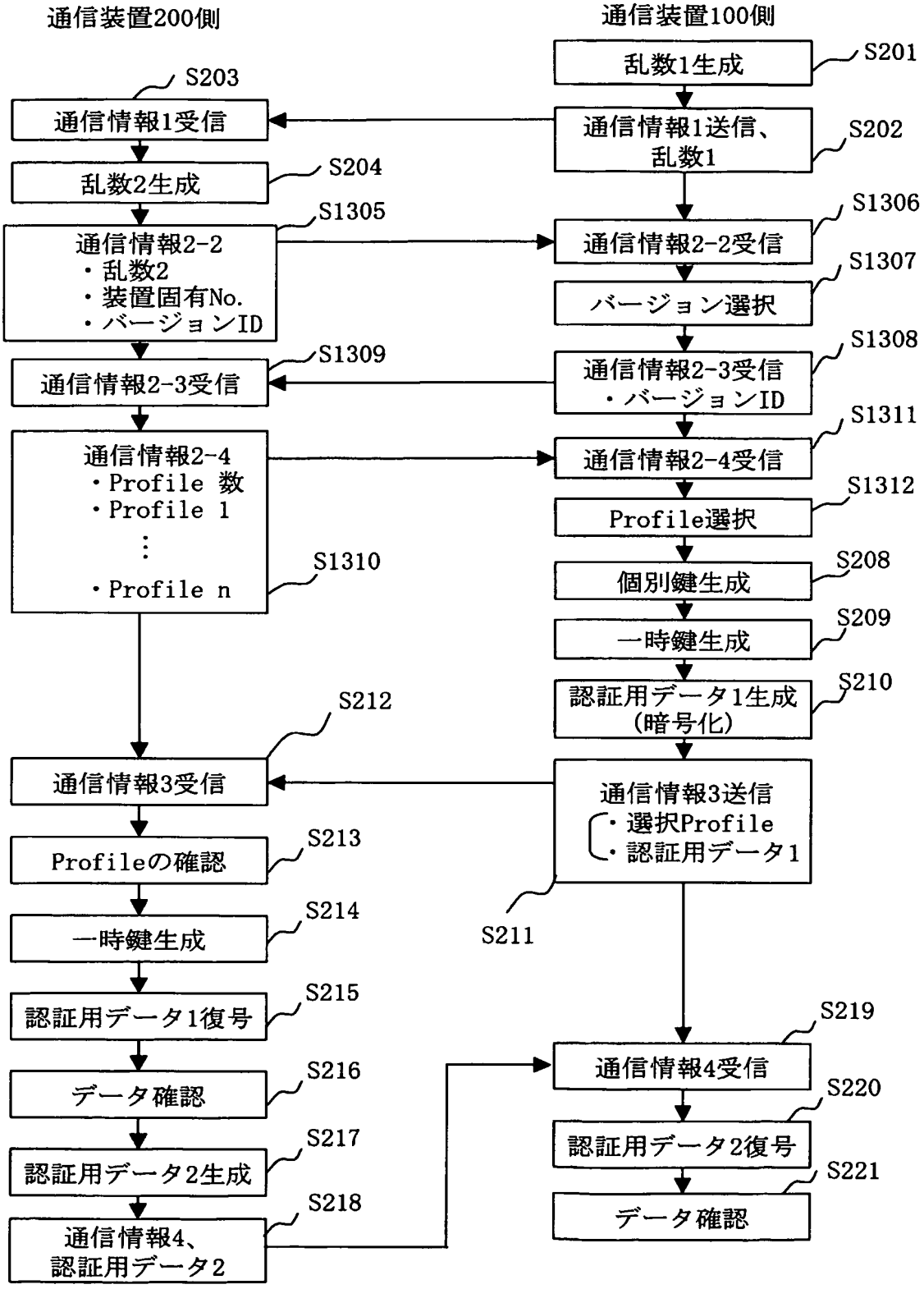
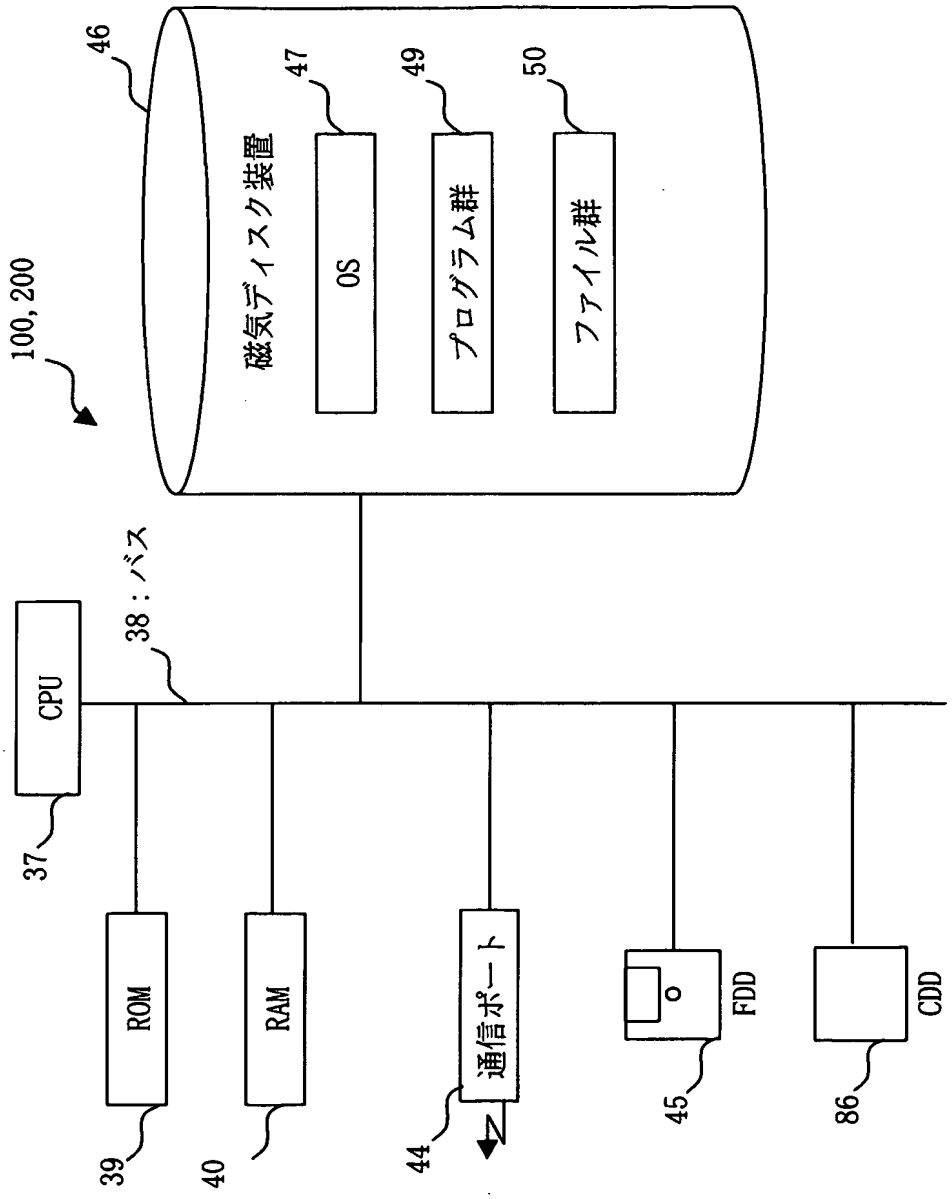

通信装置200側
通信装置100側
乱数1生成
S201
通信情報1送信、乱数1
S202
通信情報1受信
S203
乱数2生成
S204
通信情報2-2
・乱数2
・装置固有No.
・バージョンID
S1305
通信情報2-2受信
S1306
バージョン選択
S1307
通信情報2-3受信
・バージョンID
S1308
通信情報2-3受信
S1309
通信情報2-4
・Profile 数
・Profile 1
・Profile n
S1310
通信情報2-4受信
S1311
Profile選択
S1312
個別鍵生成
S208
一時鍵生成
S209
認証用データ1生成(暗号化)
S210
通信情報3送信
・選択Profile
・認証用データ1
S211
通信情報3受信
S212
Profileの確認
S213
一時鍵生成
S214
認証用データ1復号
S215
データ確認
S216
認証用データ2生成
S217
通信情報4、認証用データ2
S218
通信情報4受信
S219
認証用データ2復号
S220
データ確認
S221

図14


100, 200
46
磁気ディスク装置
47
OS
49
プログラム群
50
ファイル群
38：バス
CPU
37
ROM
39
RAM
40
通信ポート
44
FDD
45
CDD
86

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/005881

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/14, H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/14, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 11-274999 A (Hitachi, Ltd.), 08 October, 1999 (08.10.99), Figs. 5, 6 (Family: none)	1-10
Y	JP 2003-198530 A (Mitsubishi Electric Corp.), 11 July, 2003 (11.07.03), Figs. 9, 10 (Family: none)	1-10
Y	JP 9-83509 A (Hitachi, Ltd.), 28 March, 1997 (28.03.97), Figs. 4, 5 (Family: none)	1-10

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 22 July, 2004 (22.07.04)	Date of mailing of the international search report 10 August, 2004 (10.08.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/005881

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2000-293717 A (Matsushita Electric Industrial Co., Ltd.), 20 October, 2000 (20.10.00), Fig. 1 & EP 1043693 A	1-10
A	JP 2000-151578 A (Mitsubishi Electric Corp.), 30 May, 2000 (30.05.00), Full text (Family: none)	1-10
A	JP 2000-261427 A (Toshiba Corp.), 22 September, 2000 (22.09.00), Full text & EP 1035684 A	1-10
A	JP 11-328460 A (Mitsubishi Heavy Industries, Ltd.), 30 November, 1999 (30.11.99), Full text (Family: none)	1-10
A	JP 11-339080 A (Mitsubishi Heavy Industries, Ltd.), 10 December, 1999 (10.12.99), Full text (Family: none)	1-10

国際調査報告	国際出願番号　PCT／JP2004／005881

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　H04L 9／14，H04L 9／32

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　H04L 9／14，H04L 9／32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　1922－1996年
日本国公開実用新案公報　1971－2004年
日本国登録実用新案公報　1994－2004年
日本国実用新案登録公報　1996－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 11－274999 A（株式会社日立製作所） 1999．10．08，第5，6図　（ファミリーなし）	1－10
Y	JP 2003－198530 A（三菱電機株式会社） 2003．07．11，第9，10図　（ファミリーなし）	1－10
Y	JP 9－83509 A（株式会社日立製作所） 1997．03．28，第4，5図　（ファミリーなし）	1－10

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
22．07．2004	10.8.2004

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	石田　信行	5M	9469
	電話番号　03－3581－1101　内線　3598		

様式PCT／ISA／210（第2ページ）（2004年1月）

C（続き）. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2000－293717 A（松下電器産業株式会社） 2000．10．20，第1図 & EP 1043693 A	1－10
A	JP 2000－151578 A（三菱電機株式会社） 2000．05．30，全文 （ファミリーなし）	1－10
A	JP 2000－261427 A（株式会社東芝） 2000．09．22，全文 & EP 1035684 A	1－10
A	JP 11－328460 A（三菱重工業株式会社） 1999．11．30，全文 （ファミリーなし）	1－10
A	JP 11－339080 A（三菱重工業株式会社） 1999．12．10，全文 （ファミリーなし）	1－10